

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

RAYMOND MASSUD, Individually, )  
and on Behalf of All Others ) Case No.  
Similarly Situated, )  
Plaintiff, )  
v. ) **JURY TRIAL DEMANDED**  
MIDWEST GAMING & )  
ENTERTAINMENT, LLC d/b/a )  
RIVERS CASINO )  
Defendant. )

**CLASS ACTION COMPLAINT**

Plaintiff Raymond Massud (“Plaintiff”), through his undersigned counsel, brings this action against Midwest Gaming & Entertainment, LLC d/b/a Rivers Casino (“Rivers” or “Defendant”) pursuant to the investigation of his attorneys, personal knowledge as to himself and his own acts and otherwise upon information and belief, and alleges as follows:

**INTRODUCTION**

1. Rivers is a casino in Des Plaines, Illinois.
2. On or about November 20, 2023, Rivers announced that it had been involved in a “potential ransomware incident” affecting an as-yet undisclosed number of people (the “Data Breach”)<sup>1</sup>. This hacking incident was a hack and exfiltration of Rivers’ customer information.

---

<sup>1</sup> See <https://apps.web.maine.gov/online/aevIEWER/ME/40/dbfe4012-3523-4af3-8be8-f8673bd8aa0a.shtml>, last accessed November 29, 2023.

3. Rivers subsequently reported that this sensitive personal information (“SPI”) included at least “first and last name, driver’s license and/or government ID number, financial account number, and Social Security number.”<sup>22</sup>

4. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, including theft of their health insurance information.

5. The information stolen in cyber-attacks allows the modern thief to assume victims’ identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using your credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims’ names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

6. Plaintiff’s and Class members’ SPI was compromised due to Defendant’s negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiff and Class members.

7. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of Defendant’s failure to: (i) adequately protect consumers’ SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the

---

<sup>22</sup> *Id.*

“Class”). Defendant’s conduct amounts to negligence and violates state statutes.

9. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant’s conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly an increased risk to their SPI, which remains in Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

#### **JURISDICTION AND VENUE**

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant’s principal places of business is located within this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

#### **PARTIES**

13. Plaintiff Raymond Massud is a natural person residing in the St. Louis, Missouri. On or about November 27, 2023, Plaintiff was informed by letter that he had been a victim of the Data Breach.

14. Defendant Midwest Gaming & Entertainment, LLC d/b/a Rivers Casino is a for-profit Delaware limited liability corporation with its principal place of business at 900 N. Michigan Ave., Suite 1600, Chicago, Illinois. On information and belief, Defendant is a wholly-owned subsidiary of Rush Street Gaming, LLC, a Delaware limited liability corporation with its principal place of business at the same address.

#### **FACTUAL ALLEGATIONS**

15. Defendant is a casino in Des Plaines, Illinois.

16. In the ordinary course of doing business with Defendant, customers provide Rivers with SPI such as:

- a. Contact and account information, such as name, usernames, passwords, address, telephone number, email address, and household members;
- b. Social Security number, and/or drivers license number; and
- c. Payment information, such as credit card, debit card, and/or bank account number.

17. On or about November 20, 2023, Defendant began sending out letters to customers and state attorneys general stating that “On August 12, 2023, Rivers Casino became aware of suspicious activity on its systems involving a potential ransomware incident. Upon identifying the activity, Rivers Casino acted quickly to contain the threat, investigate, and ensure the security of its systems with the assistance of third-party forensic specialists. The investigation revealed that an unauthorized actor gained access to Rivers Casino’s systems on or around August 12, 2023, and as a result likely obtained some information.”<sup>3</sup>

18. Notably, the notification letters do not give greater specificity as to how this information was stolen nor what steps Rivers has taken to prevent future use. Rivers merely says,

---

<sup>3</sup> *Id.*

“We promptly engaged third-party cybersecurity support to assist with containing the incident and to help ensure the security of our systems. Further, we immediately launched an investigation in consultation with law enforcement and outside cybersecurity professionals to determine the nature and scope of the incident.”<sup>4</sup>

19. Of concern, while Defendant became aware of the Data Breach no later than August 13, 2023, it took more than three months for Defendant to notify customers and to publicly reveal the breach.

20. As a result, Plaintiff’s and class members’ SPI was in the hands of hackers for at least three months before Defendant began notifying them of the Data Breach.

21. Defendant has offered no assistance to Plaintiff or Class members beyond twelve months of credit monitoring.

22. This response is entirely inadequate to Plaintiff and Class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

23. Rivers has a privacy policy on its website.<sup>5</sup> It enumerates a long list of ways in which it may choose to share its customers’ data, though dissemination to third-party hackers is not among those with whom it may choose to share data.

24. Plaintiff and members of the Class did not so consent to having their SPI disclosed in such a manner as part of the Data Breach.

25. Defendant had obligations created by contract, industry standards, common law,

---

<sup>4</sup> *Id.*

<sup>5</sup> <https://www.riverscasino.com/desplaines/privacy-policy>, last accessed November 29, 2023.

and public representations made to Plaintiff and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

26. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the healthcare industry preceding the date of the breach.

27. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

28. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.<sup>6</sup> Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.<sup>7</sup>

29. The SPI of Plaintiff and members of the Class was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

30. Defendant knew, or reasonably should have known, of the importance of

---

<sup>6</sup> See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), <https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf>, last accessed November 29, 2023.

<sup>7</sup> The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

safeguarding the SPI of Plaintiff and members of the Class, including dates of birth and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class a result of a breach.

31. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

32. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the Class.

33. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

34. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

35. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

on the network; and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

38. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant’s cybersecurity practices.

39. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

40. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

41. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to

\$200, and bank details have a price range of \$50 to \$200.<sup>8</sup>

42. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

43. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office (“GAO”) Report to Congressional Requesters:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>9</sup>

44. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A “cyber black-market” exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

45. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim’s name but with another’s picture, and/or using the victim’s information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

46. Among other forms of fraud, identity thieves may obtain driver licenses,

---

<sup>8</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>, last accessed November 29, 2023.

<sup>9</sup> See <https://www.gao.gov/assets/gao-07-737.pdf> (June 2007) at 29, last accessed November 29, 2023.

government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

#### **FACTS SPECIFIC TO PLAINTIFF**

47. On or about November 27, 2023, Plaintiff was notified via letter from Defendant that Plaintiff's SPI had been taken as part of the Data Breach.

48. Since the time of the Data Breach, Plaintiff has received numerous emails and calls from various scammers attempting to get him to sign up various scams. This activity indicates that his information has been placed into the hands of hackers and has already been sold throughout the dark web.

49. Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in his own control.

#### **CLASS ACTION ALLEGATIONS**

50. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendant on or about November 20, 2023.

51. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

52. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

53. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. At this time, the number of class members is unknown, though Defendant has identified to the Maine Attorney General that at least 202 Maine residents have been identified. Given the regional nature of Defendant's business, the total number of impacted individuals may be in the hundreds of thousands. The Class is readily identifiable within Defendant's records.

54. **Commonality:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual members of the Class. These include:

- a. When Defendant actually learned of the Data Breach and whether its response was adequate;
- b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;
- c. Whether Defendant breached that duty;
- d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Class;
- e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Class;
- f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the SPI of Plaintiff and members of the Class secure and to prevent loss or misuse of that SPI;
- g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- h. Whether Defendant caused Plaintiff and members of the Class damage;
- i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Class that their SPI had been compromised; and
- j. Whether Plaintiff and the other members of the Class are entitled to credit monitoring and other monetary relief.

55. **Typicality:** Plaintiff's claims are typical of those of the other members of the Class

because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

56. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

57. **Superiority and Manageability:** Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual member of the Class are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

58. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as the California Subclass as a whole.

59. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

**FIRST CLAIM FOR RELIEF**  
**Negligence**  
**(By Plaintiff Individually and on Behalf of the Class)**

60. Plaintiff hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 59.

61. Defendant routinely handles SPI that is required of their customers, such as Plaintiff.

62. By collecting and storing the SPI of its customers, Defendant owed a duty of care to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

63. Defendant is aware of that duty of care to the SPI of its customers.

64. Defendant has full knowledge of the sensitivity of the SPI and the types of harm that Plaintiff and Class Members could and would suffer if the SPI were wrongfully disclosed.

65. Defendant knew or reasonably should have known that its failure to exercise due care in the collecting, storing, and using of their customers' SPI involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

66. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in

Defendant's possession was adequately secured and protected.

67. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' SPI.

68. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

69. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the SPI of Plaintiff and the Class, the critical importance of providing adequate security of that SPI, and the necessity for encrypting SPI stored on Defendant's systems.

70. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' SPI, including basic encryption techniques freely available to Defendant.

71. Plaintiff and the Class Members had no ability to protect their SPI that was in, and possibly remains in, Defendant's possession.

72. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

73. Defendant had and continues to have a duty to adequately disclose that the SPI of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice

was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

74. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiff and Class Members.

75. Defendant has admitted that the SPI of Plaintiff and Class Members was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

76. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiff and Class Members during the time the SPI was within Defendant's possession or control.

77. Defendant improperly and inadequately safeguarded the SPI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

78. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the SPI it had in its possession in the face of increased risk of theft.

79. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the SPI of patients of its customers.

80. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

81. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the SPI of Plaintiff and Class Members would not have been compromised.

82. There is a close causal connection between Defendant's failure to implement security measures to protect the SPI of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' SPI was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

83. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI of its employees and former employees in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as a result of the Data Breach for the remainder of Plaintiff's and Class Members' lives.

84. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long

as Defendant fails to undertake appropriate and adequate measures to protect the SPI in its continued possession.

**SECOND CLAIM FOR RELIEF**  
**BREACH OF IMPLIED CONTRACT**  
**(By Plaintiffs Individually and on Behalf of the Class)**

85. Plaintiff incorporates by reference all previous allegations in paragraphs 1 through 59 as though fully set forth herein.

86. Plaintiffs and Class members were required to provide their SPI to Defendant as a condition of doing business with Defendant.

87. Plaintiff and the Class entrusted their SPI to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

88. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

89. Implicit in the agreement between Plaintiffs and Class Members and the Defendants to provide SPI, was the latter's obligation to: (a) use such SPI for business purposes only, (b) take reasonable steps to safeguard that SPI, (c) prevent unauthorized disclosures of the SPI, (d) provide Plaintiffs and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their SPI, (e) reasonably safeguard and protect the SPI of Plaintiff and Class members from unauthorized disclosure or uses, (f) retain the SPI only under conditions that kept such information secure and confidential.

90. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

91. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their SPI as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their SPI to Defendant.

92. In accepting the SPI of Plaintiff and Class members, Defendant understood and agreed that it was required to reasonably safeguard the SPI from unauthorized access or disclosure.

93. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiff and Class members that they would only disclose SPI under certain circumstances, none of which relate to the Data Breach.

94. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class members' SPI would remain protected.

95. Plaintiff and Class members paid money and provided their SPI to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

96. Plaintiff and Class members would not have entrusted their SPI to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

97. Plaintiff and Class members would not have entrusted their SPI to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

98. Plaintiff and Class members fully and adequately performed their obligations under the implied contracts with Defendants.

99. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

100. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

101. Plaintiff and Class members are entitled to compensatory, consequential, and

nominal damages suffered as a result of the Data Breach.

102. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

**THIRD CLAIM FOR RELIEF**  
**Unjust Enrichment, in the Alternative**  
**(By Plaintiff Individually and on Behalf of the Class)**

103. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 59.

104. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

105. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

106. The benefits given by Plaintiff and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

107. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

108. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

109. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

**FOURTH CLAIM FOR RELIEF**  
**Invasion of Privacy**  
**(By Plaintiff Individually and on Behalf of the Class)**

110. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 59.

111. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential SPI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

112. Defendant owed a duty to its customers, including Plaintiff and the Class, to keep this information confidential.

113. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiff's and Class Members' SPI is highly offensive to a reasonable person.

114. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff's and the Class disclosed their sensitive and confidential information to Rivers as part of their business with Riverst, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

115. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

116. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

117. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

118. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

119. As a proximate result of Defendant's acts and omissions, the private and sensitive SPI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

120. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their SPI are still maintained by Defendant with their inadequate cybersecurity system and policies.

121. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the SPI of Plaintiff and the Class.

122. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

**PRAAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of himself and all Class Members, requests judgment

against the Defendant and the following:

- A. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' SPI;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;
  - iv. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);
  - v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct

- testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
  - vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
  - viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
  - ix. requiring Defendant to conduct regular database scanning and securing checks;
  - x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
  - xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in

- response to a breach;
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
  - xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
  - xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
  - xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
  - xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

- D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For pre- and postjudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

**JURY DEMAND**

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: November 29, 2023

Respectfully Submitted,

By: /s/ *Carl V. Malmstrom*  
Carl V. Malmstrom  
**WOLF HALDENSTEIN ADLER**  
**FREEMAN & HERZ LLC**  
111 W. Jackson Blvd., Suite 1700  
Chicago, Illinois 60604  
Tel: (312) 984-0000  
Fax: (212) 686-0114  
[malmstrom@whafh.com](mailto:malmstrom@whafh.com)

*Attorney for Plaintiff and  
the Putative Class*